B7

SHUSAKU YAMAMOTO

Japanese Patent No. 2835433

(Translation)

Japanese Patent No. 2835433

Issuance date: December 14, 1998
Registration date: October 9, 1998
Application number: 8-56966
Divisional application: divisional application based on:
Japanese Application No. 59-213688
Filing date: October 11, 1984
Laid-open publication number: 9-153890
Laid-open publication date: June 10, 1997
Request for examination filed on: March 21, 1996

The patentee is prepared to assign or license the patent right.

Patentee: Yutaka TSUKAMOTO

Inventor: Yutaka TSUKAMOTO

[Title of the Invention] Access control method, and authentication system and device

1. An access control method for performing access control, by which an access demanding side generates authentication data which changes dynamically by utilizing commonly changing data which commonly changes both in the access demanding side and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data, and performs authentication, the method comprising:

a data generation step of, in the access demanding side, generating the authentication data by utilizing time

variable data which varies in accordance with time counted by a device having a clock function as the commonly changing data;

a receiving step of, in the authenticating side, receiving the authentication data generated in the data generation step and transferred by data communication;

a determination step of, in the authenticating side, determining whether the authentication data received in the receiving step is appropriate or not by using the time variable data which varies in accordance with time as the commonly changing data and performing authentication; and

an access permission step of, when the authentication data is determined to be appropriate in the determination step, outputting a determination that an access by the access demanding side is permissible,

wherein, when an error occurs in the time variable data by a malfunction of the device having a clock function, automatic error correction processing is performed for automatically correcting the error so that accumulation of the error as time passes can be prevented.

2. An access control method for performing access control, by which an access demanding side generates authentication data which changes dynamically by utilizing commonly changing data which commonly changes both in the access demanding side and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data, and performs authentication, the method comprising:

a data generation step of, in the access demanding side, generating the authentication data by utilizing time variable data which varies in accordance with time counted by a device having a clock function as the commonly changing data;

a receiving step of, when the access demanding side transfers data for accessing by data communication, receiving the data in the authenticating side;

a determination step of, when the authentication data generated in the data generation step is received in the receiving step, determining in the authenticating side whether the received authentication data is appropriate or not by using the time variable data which varies in accordance with time as the commonly changing data, and performing authentication; and

an access permission step of, when the authentication data is determined to be appropriate in the determination step, outputting a determination that an access by the access demanding side is permissible,

wherein the authentication data can be determined to be appropriate in the determination step on the conditions that it is determined that a predetermined interval time period has been passed from a preceding access time to a present access time based on a data receiving status in the receiving step.

3. An authentication system for access control, by which an access demanding side to be authenticated generates authentication data which changes dynamically by utilizing commonly changing data which commonly changes both in the side to be authenticated and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data, and performs authentication, the system comprising:

clock means having a clock function;

data generation means for, in the side to be authenticated, generating the authentication data by utilizing time variable data which varies in accordance with time counted by the clock means as the commonly changing data;

data receiving means for receiving the generated authentication data by the data generation means and transferred by data communication to the authenticating side;

determination means for determining whether the authentication data received by the receiving means is appropriate or not by using the time variable data which varies in accordance with time as the commonly changing data, and performing authentication; and

automatic error correction means for, when an error occurs in the time variable data by a malfunction of the clock means, for automatically correcting the error so that accumulation of the error as time passes can be prevented.

4. An authentication system for access control, by which an access demanding side to be authenticated generates authentication data which changes dynamically by utilizing commonly changing data which commonly changes both in the side to be authenticated and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data, and performs authentication, the system comprising:

clock means having a clock function;

data generation means for, in the side to be authenticated, generating the authentication data by utilizing time variable data which varies in accordance with time counted by the clock means as the commonly changing data;

data receiving means for, when the side to be authenticated transfers data to obtain authentication to the authenticating side by data communication, receiving the data; and

determination means for, when the data receiving means receives the authentication data generated by the data generation means, determining whether the received authentication data is appropriate or not by using the time variable

data which varies in accordance with time as the commonly changing data, and performing authentication,

wherein the determination means can determine that the authentication data is appropriate on the conditions that it is determined that a predetermined interval time period has been passed from a preceding authentication time to a present authentication time based on a data receiving status by the data receiving means.

5. A personal calculation apparatus, used for an access control method for performing access control, by which an access demanding side generates authentication data which changes dynamically by utilizing commonly changing data which commonly changes both in the access demanding side and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data, and performs authentication, the personal calculation apparatus being owned by the access demanding side,

the personal calculation apparatus comprising:

data generation means, having a clock function, for generating the authentication data by utilizing time variable data which varies in accordance with time counted by the clock means as the commonly changing data; and

data output means for externally outputting the authentication data generated by the data generation means,

wherein the personal calculation apparatus having a time display function for displaying present time utilizing a counting operation of the clock function.

6. A personal calculation apparatus, used for an access control method for performing access control, by which an access demanding side generates authentication data which changes dynamically by utilizing commonly changing data

which commonly changes both in the access demanding side and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data, and performs authentication, the personal calculation apparatus being owned by the access demanding side,

the personal calculation apparatus comprising:

data generation means, having a clock function, for generating the authentication data by utilizing time variable data which varies in accordance with time counted by the clock means as the commonly changing data; and

data output means for externally outputting the authentication data generated by the data generation means,

wherein the data generation means receives time standard radio wave by code/data broadcasting and uses time variable data in accordance with the counting operation utilizing the standard time as the commonly changing data.

7. An authentication apparatus used for an access control method, by which an access demanding side generates authentication data which changes dynamically by utilizing commonly changing data which commonly changes both in the access demanding side and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data, and performs authentication, the authentication device determining whether the authentication data transferred from the access demanding side is appropriate or not and performing authentication, the authentication device comprising:

data receiving means for, when the access demanding side transfers data for accessing by data communication, receiving the data; and

determination means for, when the data receiving means receives the authentication data generated by the data generation means, determining whether the received authentication data is appropriate or not by using time variable data which varies in accordance with time as the commonly changing data, and performing authentication,

wherein the determination means can determine that the authentication data is appropriate on the conditions that it is determined that a predetermined interval time period has been passed from a preceding access time to a present access time based on a data receiving status by the data receiving means.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] The present invention relate to an access control method for, for example, limiting access to certain equipment to only certain people, and an authentication system and device used therefor. In detail, the present invention relates to an access control method and an authentication system and device, by which the access demanding side generates authentication data (password data) which dynamically changes, using commonly changing data which commonly changes both in the access demanding side and in the authenticating side and transfers the data to the authenticating side by data communication. The authenticating side determines whether the transmitted authentication data is appropriate or not, utilizing the commonly changing data and thus performing authentication.

[0002]

[Prior Art] A generally known conventional authentication system and device used for this type of access control method are described in, for example, Japanese Laid-Open Publication No. 59-154837. This conventional authentication system is structured so that authentication data (password

data) of different contents are generated between the preceding authentication time and the current authentication time and transferred to the authenticating side for the following reason. The side to be authenticated generates and transfers authentication data (password data) to the authenticating side for obtaining authentication on access control or the like. If the authentication data (password data) of the same content is generated and transferred each time, there is a risk that the authentication data (password data) is eavesdropped by a third person during the transfer and illegal access is performed. Thus, unless the authenticating side is structured to predict the manner of the dynamic change of the authentication data when the dynamically changing authentication data (password data) is transferred, the authenticating side cannot determine whether the authentication data is appropriate or not. Accordingly, the conventional authentication system is structured so that, for example, each time the side to be authenticated logs in for obtaining authentication, a sum of "1" and the preceding value is counted by the side to be authenticated and the authenticating side; and the side to be authenticated generates the dynamically changing authentication data (password data) using the counted value as the commonly changing data which commonly changes both in the side to be authenticated and the authenticating side, and transfers the data to the authenticating side by data communication. The system is structured so that the authenticating side performs authentication by determining whether the transferred authentication data (password data) is appropriate or not using the commonly changing data as a common factor.

[0003] According to one specific method by which the side to be authenticated generates the dynamically changing authentication data, for example, data including the above-mentioned commonly changing data is processed with a prescribed calculation such as encryption or the like, and the

calculation result is transferred to the authenticating side. The authenticating side is structured so that the commonly changing data is processed with a calculation such as encryption or the like by an algorithm which is common with that of the side to be authenticated, and the calculation result is compared with the transferred calculation result to determine whether they match or not, thus determining whether the data is appropriate to be authenticated or not.

[0004] Thus, this type of conventional system utilizes the commonly changing data which commonly changes both in the side to be authenticated and the authenticating side as the common factor, generates dynamically changing authentication data based on the commonly changing data, and performs authentication based on the authentication data. Accordingly, each time the side to be authenticated transfers the authentication data (password data) to the authenticating side for authentication, the content of the authentication data (password data) dynamically changes. Therefore, even if the authentication data (password data) is eavesdropped by a third person during the transfer utilizing data communication, the authentication data of a different content from the eavesdropped content is used when log-in is performed for the next authentication. Accordingly, even if that third person attempts to illegally obtain authentication for access or the like utilizing the eavesdropped authentication data, such an access is not authenticated as being appropriate. Thus, such an illegal act can be prevented.

[0005]

[0006]

[0007]

[Problems to be Solved by the Invention] This type of conventional authentication technology uses the log-in time synchronization system in which authentication data is gen-

erated using numerical value data (log-in time) obtained by updating by adding "1" to the commonly changing data which commonly changes both in the side to be authenticated and the authenticating side each time log-in is performed for authentication. Accordingly, the commonly changing data can be used as the common factor only between the side to be authenticated and specific limited authenticating side. As a result, for example, in the case where there are a plurality of authenticating sides, and one side to be authenticated logs in authenticating side A to obtain authentication and then attempts to log-in authenticating side B to obtain authentication, the commonly changing data is updated by addition of "1" as a result of the authentication by the authenticating side A, and thus the side to be authenticated and authenticating side B have different commonly changing data for the authentication by authenticating side B. Therefore, although the side to be authenticated is appropriate, it is incorrectly determined to be inappropriate. Furthermore, in the case of the log-in time synchronization system, the log-in time is updated based on the mutual communication between the side to be authenticated and the authenticating side. Accordingly, this system has an inconvenience that wrong update by a communication error is likely to occur. Moreover, in the case of the log-in time synchronization system, once the log-in time on the side to be authenticated and the authenticating side is out of synchronization, it is difficult for the authenticating side to determine whether an inappropriate access demander (side to be authenticated) is eavesdropping the authentication data (password data) and illegally accessing using the eavesdropped data, or an appropriate access demander (side to be authenticated) is accessing but the number of log-in is out of synchronization by some cause such as a communication error or the like. It is predicted that it will be difficult to recover the synchronization of the log-in time once it is put out of synchronization in the to-be-authenticated side

and the authenticating side. In other words, according to the authentication system by the conventional log-in time synchronization system, the communication is performed between the side to be authenticated and the authenticating side caused by the act of log-in of the side to be authenticated, and as a result the log-in time is updated by both sides. Such update based on the interaction of both sides raises the above-mentioned various defects.

[0008] The present invention has been conceived in light of such circumstances. An objective of the inventions defined by claims 1 through 7 is to prevent the inconveniences of the log-in time synchronization system by using, as the commonly changing data which commonly changes both in the side to be authenticated and the authenticating side, data which changes by an objective parameter which is not directly related to the act of log-in of the side to be authenticated.

[0009]

[Means for Solving the Problems] The first invention is an access control method for performing access control, by which an access demanding side generates authentication data which changes dynamically by utilizing commonly changing data which commonly changes both in the access demanding side and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data, and performs authentication, the method comprising: a data generation step of, in the access demanding side, generating the authentication data by utilizing time variable data which varies in accordance with time counted by a device having a clock function as the commonly changing data; a receiving step of, in the authenticating side, receiving the authentication data generated in the data generation step and transferred by data

communication; a determination step of, in the authenticating side, determining whether the authentication data received in the receiving step is appropriate or not by using the time variable data which varies in accordance with time as the commonly changing data and performing authentication; and an access permission step of, when the authentication data is determined to be appropriate in the determination step, outputting a determination that an access by the access demanding side is permissible, wherein, when an error occurs in the time variable data by a malfunction of the device having a clock function, automatic error correction processing is performed for automatically correcting the error so that accumulation of the error as time passes can be prevented. The second invention is an access control method for performing access control, by which an access demanding side generates authentication data which changes dynamically by utilizing commonly changing data which commonly changes both in the access demanding side and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data, and performs authentication, the method comprising: a data generation step of, in the access demanding side, generating the authentication data by utilizing time variable data which varies in accordance with time counted by a device having a clock function as the commonly changing data; a receiving step of, when the access demanding side transfers data for accessing by data communication, receiving the data in the authenticating side; a determination step of, when the authentication data generated in the data generation step is received in the receiving step, determining in the authenticating side whether the received authentication data is appropriate or not by using the time variable data which varies in accordance with time as the commonly changing data, and performing authentication; and an

access permission step of, when the authentication data is determined to be appropriate in the determination step, outputting a determination that an access by the access demanding side is permissible, wherein the authentication data can be determined to be appropriate in the determination step on the conditions that it is determined that a predetermined interval time period has been passed from a preceding access time to a present access time based on a data receiving status in the receiving step. The third invention is an authentication system for access control, by which an access demanding side to be authenticated generates authentication data which changes dynamically by utilizing commonly changing data which commonly changes both in the side to be authenticated and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data, and performs authentication, the system comprising: clock means having a clock function; data generation means for, in the side to be authenticated, generating the authentication data by utilizing time variable data which varies in accordance with time counted by the clock means as the commonly changing data; data receiving means for receiving the generated authentication data by the data generation means and transferred by data communication to the authenticating side; determination means for determining whether the authentication data received by the receiving means is appropriate or not by using the time variable data which varies in accordance with time as the commonly changing data, and performing authentication; and automatic error correction means for, when an error occurs in the time variable data by a malfunction of the clock means, for automatically correcting the error so that accumulation of the error as time passes can be prevented. The fourth invention is an authentication system for access control, by which an access demanding side to be authenti-

cated generates authentication data which changes dynamically by utilizing commonly changing data which commonly changes both in the side to be authenticated and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data, and performs authentication, the system comprising: clock means having a clock function; data generation means for, in the side to be authenticated, generating the authentication data by utilizing time variable data which varies in accordance with time counted by the clock means as the commonly changing data; data receiving means for, when the side to be authenticated transfers data to obtain authentication to the authenticating side by data communication, receiving the data; and determination means for, when the data receiving means receives the authentication data generated by the data generation means, determining whether the received authentication data is appropriate or not by using the time variable data which varies in accordance with time as the commonly changing data, and performing authentication, wherein the determination means can determine that the authentication data is appropriate on the conditions that it is determined that a predetermined interval time period has been passed from a preceding authentication time to a present authentication time based on a data receiving status by the data receiving means. The fifth invention is a personal calculation apparatus, used for an access control method for performing access control, by which an access demanding side generates authentication data which changes dynamically by utilizing commonly changing data which commonly changes both in the access demanding side and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by

utilizing the commonly changing data, and performs authentication, the personal calculation apparatus being owned by the access demanding side, the personal calculation apparatus comprising: data generation means, having a clock function, for generating the authentication data by utilizing time variable data which varies in accordance with time counted by the clock means as the commonly changing data; and data output means for externally outputting the authentication data generated by the data generation means, wherein the personal calculation apparatus having a time display function for displaying present time utilizing a counting operation of the clock function. The sixth invention is a personal calculation apparatus, used for an access control method for performing access control, by which an access demanding side generates authentication data which changes dynamically by utilizing commonly changing data which commonly changes both in the access demanding side and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data, and performs authentication, the personal calculation apparatus being owned by the access demanding side, the personal calculation apparatus comprising: data generation means, having a clock function, for generating the authentication data by utilizing time variable data which varies in accordance with time counted by the clock means as the commonly changing data; and data output means for externally outputting the authentication data generated by the data generation means, wherein the data generation means receives time standard radio wave by code/data broadcasting and uses time variable data in accordance with the counting operation utilizing the standard time as the commonly changing data. The seventh invention is an authentication apparatus used for an access control method, by which an access demanding side generates

authentication data which changes dynamically by utilizing commonly changing data which commonly changes both in the access demanding side and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data, and performs authentication, the authentication device determining whether the authentication data transferred from the access demanding side is appropriate or not and performing authentication, the authentication device comprising: data receiving means for, when the access demanding side transfers data for accessing by data communication, receiving the data; and determination means for, when the data receiving means receives the authentication data generated by the data generation means, determining whether the received authentication data is appropriate or not by using time variable data which varies in accordance with time as the commonly changing data, and performing authentication, wherein the determination means can determine that the authentication data is appropriate on the conditions that it is determined that a predetermined interval time period has been passed from a preceding access time to a present access time based on a data receiving status by the data receiving means.

[0010]

[Function] According to the first invention, by the data generation step, in the access demanding side, the authentication data is generated by utilizing time variable data which varies in accordance with time counted by a device having a clock function as the commonly changing data. By the receiving step, the authentication data generated in the data generation step and transferred by data communication is received by the authenticating side. By the determination step, in the authenticating side, it is determined

whether the authentication data received in the receiving step is appropriate or not by using the time variable data which varies in accordance with time as the commonly changing data and authentication is performed. By the access permission step, when a determination indicating appropriateness is obtained by the determination step, a determination that an access by the access demanding side is permissible is output. When an error occurs in the time variable data by a malfunction of the device having a clock function, automatic error correction processing is performed for automatically correcting the error so that over-time accumulation of the errors can be prevented. According to the second invention, by the data generation step, in the access demanding side, the authentication data is generated by utilizing time variable data which varies in accordance with time counted by a device having a clock function as the commonly changing data. By the receiving step, when the access demanding side transfers data for accessing by data communication, the data is received by the authenticating side. When the authentication data generated in the data generation step is received in the receiving step, by the determination step, in the authenticating side, it is determined whether the received authentication data is appropriate or not by using the time variable data which varies in accordance with time as the commonly changing data, and authentication is performed. By the access permission step, when a determination indicating appropriateness is obtained by the determination step, a determination that an access by the access demanding side is permissible is output. The authentication data can be determined to be appropriate in the determination step on the conditions that it is determined that a predetermined interval time period has been passed from a preceding access time to a present access time based on a data receiving status in the receiving step. According to the third invention, by the action of the data generation means, in the side to be authenticated, the authentication

data is generated by utilizing time variable data which varies in accordance with time counted by the clock means having a clock function as the commonly changing data. By the action of the data receiving means, the authentication data generated by the data generation means and transferred by data communication to the authenticating side is received. By the action of the determination means, it is determined whether the authentication data received by the data receiving means is appropriate or not by using the time variable data which varies in accordance with time as the commonly changing data, and authentication is performed. By the action of the automatic error correction means, when an error occurs in the time variable data by a malfunction of the clock means, the error is automatically corrected so that accumulation of the error as time passes can be prevented. According to the fourth invention, by the action of the data generation means, in the side to be authenticated, the authentication data is generated by utilizing time variable data which varies in accordance with time counted by the clock means having a clock function as the commonly changing data. By the action of the data receiving means, when the side to be authenticated transfers data to obtain authentication to the authenticating side by data communication, the data is received. When the authentication data generated by the data generation means is received by the data receiving means, by the action of the determination means, it is determined whether the received authentication data is appropriate or not by using the time variable data which varies in accordance with time as the commonly changing data, and authentication is performed. By the action of the determination means, a determination indicating appropriateness can be obtained on the conditions that it is determined that a predetermined interval time period has been passed from a preceding authentication time to a present authentication time based on a data receiving status by the data receiving means. According to the personal calculation apparatus of

the fifth invention, by the action of the data generation means having a clock function, the authentication data is generated by utilizing time variable data which varies in accordance with time counted by the clock means as the commonly changing data. By the action of the data output means, the authentication data generated by the data generation means is externally output. Utilizing a counting operation of the clock function, the present time is displayed. According to the personal calculation apparatus of the sixth invention, by the action of the data generation means having a clock function, the authentication data is generated by utilizing time variable data which varies in accordance with time counted by the clock means as the commonly changing data. By the action of the data output means, the authentication data generated by the data generation means is externally output. The data generation means receives time standard radio wave by code/data broadcasting and uses time variable data in accordance with the counting operation utilizing the standard time as the commonly changing data. According to the authentication apparatus of the seventh invention, by the action of the data receiving means, when the access demanding side transfers data for accessing by data communication, the data is received. When the data receiving means receives the authentication data generated by the data generation means, by the action of the determination means, it is determined whether the received authentication data is appropriate or not by using time variable data which varies in accordance with time as the commonly changing data, and authentication is performed. The determination means can determine that the authentication data is appropriate on the conditions that it is determined that a predetermined interval time period has been passed from a preceding access time to a present access time based on a data receiving status by the data receiving means.

[0011]

[Embodiments of the Invention] Before describing the embodiments of an access control system according to the present invention, embodiments of a digital signature system which will be increasingly required in data communication in a highly information-oriented society will be described.

[0012] As shown in Figure 1, a personal terminal device 3 including a built-in RAM or CPU is structured to be detachable to a data input apparatus 2 as an example of data input means having a keyboard 1 by which "hiragana" (translation note: Japanese phonetic letters) and numerals can be input by character keys and numeral keys. This personal terminal device can be any device which is individually possessed by a person sending data with an intention of performing digital signature. Conventionally and commonly known such devices include, for example, an IC card.

[0013] Figure 10 shows a circuit configuration of the personal terminal device 3 possessed by an individual. The personal terminal device 3 accommodates a CPU 50, a ROM 51, a RAM 52, and an I/O port 53. The ROM 51 stores therein an operation program of the CPU 50, i.e., a program shown in a flowchart of Figure 2 described below or the like. The CPU 50 operates in accordance with the program stored in the ROM 51, and calls a character-numeral conversion rule or a secret function as an example of a secret rule described below and causes the rule to be stored in the RAM 52. As described below, sending data which has been input from the keyboard 1 through the I/O port 53 is converted as shown in Figure 2 by an algorithm in accordance with the secret rule stored in the RAM 52. The converted data is output through the I/O port 53.

[0014] The secret rule stored in the personal terminal device 3 is constituted of, for example, a character-numeral conversion rule for converting hiragana letters into numer-

als in accordance with a certain rule, a secret function f(x) consisting of a combination of trigonometric functions and an exponential function and the like. Different types of secret rules are stored in different personal terminal devices 3. Accordingly, each of the signers attempting to sign possesses the respective personal terminal device 3 to hold his/her own secret rule. The secret rule is secret from others.

[0015] The personal terminal device 3 has the program shown in the flowchart of Figure 2 incorporated therein. For performing digital signature, sending data such as characters of an agreement to be signed or the like is input from the keyboard 1 in the form of hiragana letters while the personal terminal device 3 is attached to the input device 2. The numerals such as dates or the like are input as they are. When characters are input, each of the characters is converted into a numeral in accordance with the character-numeral conversion rule each time the character is input and the converted numerals are added together. When numerals are input, those numerals are added together. When key E for END is pressed, a sum P(n) of all the characters and numerals is substituted into the secret function f(x) and an answer is found. The converted data, which is the answer consisting of an encrypted code (numeral in this case), is output through the I/O port 53 as signature data and displayed on the display section 4. The signature data displayed on a display section 4 is sent together with the sending data such as the agreement or the like, which is the target of authentication.

[0016] The input device 2 can be a teletex terminal. In this case, the sending data to be signed is input from the keyboard of the teletex terminal to the personal terminal device 3. It is structured that the data for authentication, which is converted data output from the personal terminal

device 3, is transferred to the other party of the agreement from the teletex terminal.

[0017] The secret rule consisting of the character-numeral conversion rule and the secret function is registered in, for example, a public institution such as government offices, a service organization or the like having a duty to protect privileged information.

[0018] In the case of digital signature for performing authentication for checking, such as a document acceptance stamp, a receipt stamp, money receipt stamp or the like, the act to be authenticated such as document acceptance or the like is input in hiragana letters from the keyboard 1, and the date of the act to be authenticated is input. Thus, the converted data, i.e., signature data, is calculated. When, for example, the act to be authenticated is document acceptance and the date of authentication is October 9, 1984, 11:35 (eleven thirty-five), "しょるいうけつけ1984ねん10がつ9ひ11じ35ふん" is input from the keyboard 1. (Translation note: hiragana letters are included in the above phrase as discussed above.)

[0019] It can be structured that one-touch input is possible by allocating various representative checking acts such as document acceptance, receipt and the like to one operation key of the keyboard 1.

[0020] Needless to say, the acts of document acceptance, receipt and the like listed as the acts to be authenticated in the sense of the present invention are mere examples, and the acts to be authenticated includes various checking acts such as an act of ordering, an act of delivering a product, an act of receiving money, and the like in the case of authentication of order sheets, statements of delivery, receipts and the like.

[0021] Next, other examples will be described.
(1) Instead of using a numeral obtained by a secret function as signature data as it is, a part or the entirety of the obtained numeral is converted into characters such as hiragana letters, "katakana" (translation note: Japanese phonetic letters), Chinese characters, alphabetical letters or the like, or graphics or symbols, or combinations thereof, or combinations thereof with colors, based on a certain secret rule, to be used as signature data.

[0022] (2)The secret rule is stored in a file apparatus 5 of a corporation or the like as shown in Figure 3, instead of being stored in the personal terminal device 3. In such a case, the teletex terminal 6 and the file apparatus 5 are connected to each other through a LAN 8 or the like via a computer 7. A signer of a paperless transaction performed with another corporation utilizing public telephone lines or the like calls his/her own secret rule by operating the teletex terminal 6 and performs encryption or other conversion works by the computer 7. When the secret rule is called, an individual identification system described below is utilized to check by the computer 7 whether or not the secret rule specified by the signer really belongs to the signer. Only when the secret rule is confirmed to belong to the signer, an access of the signer to the specified secret rule is realized.

[0023] In the figure, reference numeral 9 represents a node.
(3) The signer calls his/her secret rule, from a file apparatus of a public institution, service organization or the like in which the secret rule has been registered, or from a file apparatus of his/her house through data communication, instead of from the file apparatus 5 in the corporation; and

performs encryption or other conversion works by a computer connected to the called file apparatus.

[0024] (4)The personal terminal device 3 is structured so that the encryption or other conversion function is stopped when a prescribed signal (different by transmitter to transmitter) from a signal transmitter (e.g., of a ring-shape) owned by the owner of the device cannot be received. Thus, abuse by others is prevented when the personal terminal device 3 is lost.

[0025] (5)As a conversion method such as encryption or the like, $P(N)=P(N-1)+N\cdot D(N)$, $P(N)=P(N-1)+D(N)/N$, $P(N)=P(N-1)/N+D(N)$ or $P(N)=P(N-1)/N+N\cdot D(N)$ or the like is used instead of $P(N)=P(N-1)+D(N)$ shown in Figure 2.

[0026] Next, an embodiment of an access control system according to the present invention (individual identification system) will be described. This access control system can also be utilized in order to, for example, when a secret rule is to be read, determine whether or not the specified secret rule actually belongs to the individual who specified the secret.

[0027] As shown in Figure 4, a piece of equipment which should be permitted to be accessed to a certain limited range of people, such as equipment for calling a person's own account in a bank 10, retrieving secret technological information in a data bank 11, unlocking a coin locker 12 or the like is connected via a public telephone line 15 to a computer 13 or 14 in his/her house or in a prescribed institution for performing individual identification on whether or not an equipment user (access demander) may be permitted to access the equipment. It is structured so that data communication is possible between the equipment 10, 11, 12 and the computer 13, 14 for performing the individual identifi-

cation. In the figure, reference numeral 16 represents a network control unit (NCU), and reference numeral 17 represents a switchboard.

[0028] When, for example, the technological information in the data bank 11 is demanded to be utilized, the data bank 11 is first called by a CAPTAIN terminal 18 so as to retrieve the desired technological information. When the technological information is secret technological information permitted to be used only by certain people, individual identification is performed using the following procedure.

[0029] (1) The equipment user who tries to use the technological information informs the data bank 11 of the calling number of the computer 13 or 14 in his/her house or in a prescribed institution for performing individual identification.

[0030] (2) The data bank 11 checks whether or not the number is registered beforehand and belongs to an individual who can be permitted to obtain a permission of use. If the number belongs to an individual who can be permitted to obtain a permission of use, the data bank 11 requests for transmission of the identification number. If the number does not belongs to an individual who can be permitted to obtain a permission of use, the data bank 11 does not permit the use.

[0031] (3) When the request for transmission of the identification number is issued, the equipment user transmits an identification signal output by his/her device 33 to the data bank 11 by the CAPTAIN terminal 18.

[0032] (4) The data bank 11 transmits the received identification signal to the computer 13 or 14 having the calling number. The computer 13 or 14 performs individual identification determination (described below) on whether or not the

received identification number is correct and transmits the result to the data bank 11.

[0033] (5) The data bank 11 permits an access to the specified secret technological information only when a determination result that the identification number is correct is transmitted.

[0034] Next, a procedure for unlocking the coin locker 12 is as follows. First, the calling number of the computer 13 or 14 in the equipment user's house or in a prescribed institution for performing individual identification is input by operating a keyboard on an internal surface of the door of the coin locker in an unlocked state. The door is closed and locked in the state where the computer 13 or 14 is registered beforehand and the door is set so that the computer 13 or 14 is automatically called when an unlocking operation is performed. For unlocking, the identification signal is input on an external surface of the door, and the unlocking control is performed in a similar method to that in (4) and (5) described above.

[0035] Next, a procedure for calling the user's bank account for, for example, paying money, is as follows in a cashless payment system (bank POS system) or the like, according to which only a numerical figure is transferred, i.e., money in the user's bank account is transferred to the bank account of the money recipient, without transfer of cash. First, the calling number of the computer 13 or 14 in the user's house or in a prescribed institution is registered in the bank beforehand. It is set so that the computer 13 or 14 is automatically called when the user's bank account is specifically called. For making a payment for the purchase done in a supermarket or the like, the user specifically calls his/her bank account from a register 19 of the supermarket or the like, and accesses his/her bank account in a

similar manner to that in (4) and (5) described above. As the means for specifically calling his/her bank account, the method of inputting a bank account calling and specifying signal which is output from the device 33 of the equipment user from a register 19 and transferring the signal to the bank is used.

[0036] For an access for unlocking the door of an automobile or the like, or for starting an engine, data communication by a cabled medium such as a public telephone line or the like is unusable since the equipment to be utilized is a movable object. Accordingly, a wireless medium such as satellite communication or the like is used. Thus, the "data communication" in the sense of the present invention is a broad concept including wireless media as well as cabled media.

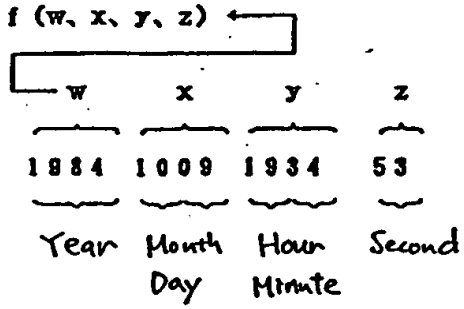
[0037] Next, the above-mentioned individual identification method will be described. As shown in Figure 5, the device 33 owned by the equipment user is constituted of a wrist watch for receiving code/data broadcasting such as a time standard radio wave by JJY or the like and displaying the time based on the received signal. The current time displayed by the wrist watch 33 is substituted, as an input signal, into a secret function (different wrist watch by wrist watch) as a secret rule which is stored in the wrist watch 33, and the answer is calculated. The answer and a part of the used input signal corresponding to the second are output as an identification signal. The output is performed as follows. First, as shown in Figure 6, a transmission button 21 is pushed, and the identification signal is sent out for a certain period of time (10 seconds) to a hand 23 from a signal transmission section 22 consisting of a conductive plate on a rear surface of the wrist watch. The identification signal is transmitted to an identification signal receiving section 24 of the register 19, the coin

locker 12, the automobile 20, the CAPTAIN terminal 18, a telephone, a teletex terminal or the like, using the hand 23, which is a conductive body, as a medium. The transmitted identification signal is transmitted to the computer 13 or 14 in the user's house or a prescribed institution for performing individual identification determination. The input signal is substituted into a secret function as a secret rule which is registered in the computer beforehand, and the answer is calculated. The answer and the identification signal are compared with each other to determine whether or not the identification signal is correct. Thus, the individual identification determination is performed.

[0038] The secret function is a function consisting of a combination of trigonometric functions, exponential functions and the like, and has four variables w, x, y and z. As in expression 1 shown below, each part of the input signal is substituted into w, x, y and z to calculate the answer.

[0039]

[Expression 1]



[0040] For sending an identification signal from a foreign country to Japan, an input signal obtained by converting the time in that foreign country into Japan time needs to be substituted into the secret function.

[0041] In the figure, reference numeral 25 represents a ring-shape signal transmitter owned by an equipment user for generating a certain signal. The signal is different transmitter by transmitter. The signal transmitter is structured so as to transmit an identification signal only when the wrist watch 33 is receiving a prescribed signal from the transmitter 25. Thus, abuse by others is prevented when the wrist watch 33 is lost.

[0042] In the figure, reference numeral 26 represents a keyboard used for calling the user's bank account or the like. A PIN is input to or a bank account calling and specifying signal is output from the keyboard. These signals are output from the signal transmission section 22 similarly to the identification signal.

[0043] The wrist watch 33 is structured so as to correct an error from the displayed time incessantly based on the signal by the code/data broadcasting. A flowchart of the program incorporated into the wrist watch 33 is shown in Figure 7. Thus, the wrist watch 33 includes a microcomputer operating in accordance with a program, i.e., a microcomputer having a similar circuit configuration as that shown in Figure 10 built therein.

[0044] The flowchart shown in Figure 7 will be briefly described. By step S (hereinafter, referred as simply to "S") 1, it is determined whether or not a time standard radio wave by the code/data broadcasting has been received. The program waits until the wave is received. When the wave is received, the program advances to S2, where an operation of correcting a frequency divider based on the time standard radio wave and displaying the corrected time is performed. Then, the program advances to S3, where it is determined whether or not a signal from a receiver 25 (see Figure 5) has been received. When the signal has not been received,

the program returns to S1. When the signal has been received, the program advances to S4, where it is determined whether or not a receiving button 21 (see Figure 6) of an individual identification signal has been turned ON. When the button has not been turned ON, the program returns to S1. When the button has been turned ON, the program advances to S5, where the process of inputting an input signal consisting of current time to each of w, x, y and z of the secret function f(w, x, y, z) and calculating the answer A is performed. Then, the program advances to S6, where the process of outputting the calculated answer A and a numerical value NZ substituted into z as identification signals is performed.

[0045] Next, a flowchart for a program incorporated into the computer 13 or 14 in which the secret rule has been registered is shown in Figure 8. The flowchart will be briefly described based on Figure 8. In S7, it is determined whether or not the identification signal A and NZ have been received. The program waits until they are received. When they are received, the program advances to S8, where it is determined whether or not the difference between the current time and NZ is within a tolerance K seconds. When the difference is not within the tolerance K seconds, the program advances to S12, where the process of outputting a determination that the access to the equipment is not permissible is performed, and the program returns to S7. The tolerance K is a delay time period obtained in consideration of the time period required to calculate the identification signal in the wrist watch 33 or the time period required for data communication to the computer 13 or 14 in which secret rule has been registered. The tolerance K is a short period of time of, for example, 3 seconds or the like.

[0046] When the difference is within the tolerance K by S8, the program advances to S9, where it is determined whether or not the tolerance K seconds or more has passed since the

preceding receiving time up to the current identification signal receiving time. When the tolerance K seconds or more has not passed, the program advances to S12, where it is determined that the access is not permissible. It is included in the conditions for permitting an access that the tolerance K seconds or more has passed since the preceding receiving time up to the current identification signal receiving time in order to prevent an inconvenience that, for the period of the tolerance K seconds after the identification signal A and NZ are transmitted, a system abuser records and transmits the identification signal A and NZ to the computer 13 or 14 in which the secret rule has been registered so as to illegally access the equipment.

[0047] When it is determined that the tolerance K seconds have passed by S9, the program advances to S10, where the process of substituting the input signal consisting of the current time into w, x, y, of the secret function f(w, x, y, z) registered beforehand, substituting the NZ into z to calculate the answer B is performed. The program advances to S11, where it is determined whether or not the B is equal to the received A. If they are not equal, the program advances to S12, where it is determined that the access is not permissible. If they are equal, the program advances to S13, where the process of outputting a determination that the access to the equipment is permissible is performed. Then, the program returns to S7.

[0048] Next, another embodiment of this individual identification system will be described.

(1) As an input signal into the secret function, a numeral, which is common nationwide or worldwide and which increases or decreases over-time based on the code/data broadcasting is used instead of the current time. In this case, the numeral for the input signal may be transmitted from a identification signal input terminal such as the register 19, the

CAPTAIN terminal 18 or the like. The transmission means to the device 33 owned by the equipment user may be either through radio wave or cable.

[0049] Furthermore, the device 33 owned by the equipment user is not limited to a wrist watch and may be any individual terminal such as a handheld electronic calculator or the like.

[0050] (2) As means for selecting an unused signal to be used as the input signal, a function for rejecting an input signal which has been used in the past is added to computer 13 or 14 in which the secret rule has been registered. A flowchart of a program to be incorporated into the computer 13 or 14 in which the secret rule has been registered and a flowchart of a program to be incorporated into the device 33 owned by the equipment user in such a case are respectively shown in Figure 9(A) and (B).

[0051] The flowcharts shown in Figure 9(A) and (B) will be briefly described. First, the program incorporated into the device 33 owned by the equipment user will be described based on Figure 9(B). In S22, the initial value of I is set to "1". Then, the program advances to S23, where it is determined whether the transmission button 21 (see Figure 6) has been turned ON or not. The program waits until the transmission button 21 is turned ON. When the transmission button 21 is turned ON, the program advances to S24, where the process of substituting the I into the secret function f(x) and calculating the value A of f(I) is performed. At this stage, the I is "1". Next, the program advances to S25, where the process of outputting the respective values of A and I as identification signals is performed. The program advances to S26, where the process of adding "1" to the current value of I to make a new value of I is performed. Thereafter, the program returns to S23.

[0052] Thus, in the case where the first access is attempted using the device 33 owned by the equipment user, the identification signal A calculated by substituting I=1 into the f(I) is transferred to the computer 13 or 14 in which the secret rule has been registered. In the case where the second access is attempted, I=2 when the transmission button 21 of the device 33 owned by the equipment user is turned ON to calculate the identification signal A. Therefore, the identification signal A calculated by substituting I=2 into f(I) is transferred.

[0053] Thus, in the device 33, each time the transmission button 21 is turned ON to perform an access operation, I is updated as a result of addition of "1". Therefore, each time an access operation is performed, a different value of I is used. As a result, a different identification signal A is calculated and transferred each time.

[0054] Next, the program incorporated into the computer 13 or 14 in which the secret rule has been registered will be described based on Figure 9(A). By S14, the initial value of J is set to "1". The program advances to S15, where it is determined whether the identification signals A and I transferred from the device 33 have been received or not, and the program waits until they are received. When they are received, the program advances to S16, where it is determined whether J=I or not. During the first access operation, J is "1" and I should be "1". Therefore, it should be determined to be YES by S16. However, a person who attempts to illegally access the equipment cannot decide the current value of I. Accordingly, it is considered that he/she substitutes an arbitrary value to I and transfers the value to the computer 13 or 14. In such a case, it is determined to be NO by S16. The program advances to S17, where the process of outputting a determination that the access to the

equipment is not permissible is performed, and the program returns to S15.

[0055] When it is determined that J=I, the program advances to S18, where the process of substituting J into the registered secret function f(x) to calculate the answer B is performed. Then, the program advances to S19, where it is determined whether the calculated B and the transferred A are equal to each other or not. When they are not equal, the program advances to S17, where it is determined that the access to the equipment is not permissible. When they are equal, the program advances to S20, where the process of outputting a determination that the access to the equipment is permissible is performed. Then, the program advances to S21, where the process of updating J by adding "1" to the current value of J is performed, and then the program returns to S15.

[0056] Thus, the computer 13 or 14 in which the secret rule has been registered updates the value of J by adding "1" each time the identification signals A and I are transferred from the device 33. As a result, the current value of I in the device 33 and the current value of J in the computer 13 or 14 in which the secret rule has been registered should be in synchronization with each other and identical.

[0057] (3) It is structured that a secret rule of a person who is the subject of the manipulation such as a fugitive or the like is registered and when an identification signal is transferred to a computer in which the secret rule has been registered, a signal instructing to notify the location is returned to the terminal to which the identification signal was input, and a signal indicating the location where the terminal is installed is transferred from the terminal to a computer of the police.

[0058] (4) As the secret rule used for the individual identification, a secret rule used for the above-described invention of digital signature is used. In other words, a secret rule owned by a person is used both for the digital signature system and the individual identification system.

[0059] Next, the various embodiment described above will be listed below.
(1) In the individual identification system (access control system), a function of rejecting an input signal which has been used in the past is provided to the determination means as the means for selecting an unused signal to be used.

[0060] (2) In the individual identification system, a numeral which is common nationwide and increases or decreases whenever selected to be used or over-time is used as the input signal as the means for selecting an unused signal to be used.

[0061] (3) In the individual identification system described in (2) above, the numeral is defined based on the signal transferred by the code/data broadcasting.

[0062] (4) In the individual identification system described in (2) or (3) above, the numeral represents the current year, month, day and time.

[0063] (5) In the individual identification system described in (2) above, the device of the equipment user is constituted of a wrist watch, and the time displayed by the wrist watch is used as the input signal.

[0064] (6) In the individual identification system described in (5) above, the wrist watch can display time based on the signal transferred by the code/data broadcasting.

[0065] (7)In the individual identification system described in (3) or (6) above, the code/data broadcasting is transmitted from individual piece of equipment which are the targets of utilization.

[0066] (8)In the individual identification system described in (5) or (6) above, the wrist watch has a signal transmission section to the human hand so as to transfer the output identification signal to the equipment which is the target of utilization via the human hand as the medium.

[0067] (9)In the individual identification system, the device owned by the equipment user is structured to stop the function for individual identification when a prescribed signal from the signal transmitter owned by the owner of the device cannot be received.

[0068] Next, the correspondence between the elements of present invention and the above-described embodiments will be described. Secret conversion data specific to an access demander is constituted by the secret function f(w, x, y, z) or f(I), f(x) shown in Figure 9. A personal calculation device storing the secret conversion data specific to an access demander is constituted by the device 33 owned by the equipment user. As described above, variable data which is used both in the personal calculation device and for the access permission or denial determination means (described below) and which is variable between the preceding access time and the present access time is constituted by the current time shown in S5 of Figure 7 and S10 of Figure 8, or I shown in S24 of Figure 9 and J shown in S18. As described above, the personal calculation device has an operation function for converting the above-selected variable data by a prescribed algorithm in accordance with the secret conversion data.

[0069] The access permission or denial determination means for determining whether an access is permitted or not is constituted by the computer 13 or 14 in which the secret rule has been registered. As described above, the converted data obtained by the conversion by the personal calculation device (identification signal such as A or the like) is transferred to the access permission or denial determination means by the data communication (see Figure 4). The access permission or denial determination means determines whether the transferred converted data is appropriate or not based on the above-selected conversion data.

[0070] The device having a clock function (clock means) is constituted by the wrist watch 33. The time variable data, which is commonly changing data which commonly changes both in the side to be authenticated (access demanding side) and the authenticating side and varies in accordance with time, is constituted by the input signal consisting of the present time in S5 of Figure 7 and the input signal consisting of the present time in S10 of Figure 8. The data generation step of, in the access demanding side, generating the authentication data by using time variable data which varies in accordance with time counted by a device having a clock function as the commonly changing data is constituted by S1, S2 and S5 of Figure 7. The data generation means for, in the side to be authenticated, generating the authentication data by using time variable data which varies in accordance with time counted by the clock means as the commonly changing data is constituted by S1, S2 and S5 of Figure 7. The receiving step (data receiving means) is constituted by S7 of Figure 8. The hardware circuit of the computer 13, 14 may be a general computer hardware circuit as shown in Figure 10. The determination step of, in the authenticating side, determining whether the authentication data received in the receiving step is appropriate or not by using the time variable data which varies in accordance with time as

the commonly changing data and performing authentication is constituted by S9, S10 and S11 of Figure 8. The determination means for determining whether the authentication data received in the receiving step is appropriate or not by using the time variable data which varies in accordance with time as the commonly changing data and performing authentication is constituted by S9, S10 and S11 of Figure 8. The automatic error correction processing, for when an error occurs in the time variable data by a malfunction of a device having a clock function, for automatically correcting the error so that over-time accumulation of the errors can be prevented is constituted by S1 and S2 of Figure 7. The automatic error correction means, for when an error occurs in the time variable data by a malfunction of the clock means, for automatically correcting the error so that over-time accumulation of the errors can be prevented is constituted by S1 and S2 of Figure 7. The access permission step of, when a determination indicating appropriateness is obtained by the determination step, outputting a determination that an access by the access demanding side is permissible is constituted by S13 of Figure 8. The personal calculation apparatus used for an access control method, by which an access demanding side generates authentication data which changes dynamically by utilizing commonly changing data which commonly changes both in the access demanding side and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data and performs authentication and performs access control, the personal calculation apparatus being owned by the access demanding side, is constituted by the writs watch 33. The authentication apparatus used for an access control method, by which an access demanding side generates authentication data which changes dynamically by utilizing commonly changing data which commonly

changes both in the access demanding side and an authenticating side, and transfers the generated authentication data to the authenticating side by data communication; and the authenticating side determines whether the transferred authentication data is appropriate or not by utilizing the commonly changing data and performs authentication, the authentication apparatus determining whether the authentication data transferred from the access demanding side is appropriate or not to perform authentication, is constituted by the computer 13, 14.

[0071]

[Effect of the Invention] According to the first invention, the authentication data is changed while maintaining the synchronization between the access demanding side and the authenticating side. The authentication data is updated in synchronization by utilizing, as the common factor, time variable data which varies in accordance with an objective parameter of time, which is common nationwide. Accordingly, the above-described inconvenience of the log-in number synchronization system that the commonly changing data of both sides are put out of synchronization can be prevented to a maximum degree. Since the error in the time variable data caused by the malfunction of the device having a clock function is automatically corrected, the inconvenience that the errors in the time variable data are gradually accumulated and the both sides are put out of synchronization can be prevented to a maximum degree. According to the second invention, the authentication data is changed while maintaining the synchronization between the access demanding side and the authenticating side. The authentication data is updated in synchronization by utilizing, as the common factor, time variable data which varies in accordance with an objective parameter of time, which is common nationwide. Accordingly, the above-described inconvenience of the log-in number synchronization system that the commonly changing data

of both sides are put out of synchronization can be prevented to a maximum degree. In the case of the time variable data, when the access demander, demanding access, logs in consecutively in a short period of time, i.e., when much time has not been passed since the preceding access up to the present access, the authentication data used for the preceding access can have almost the same content with that of the authentication data used for the present access. Especially when the log-in is performed consecutively within a minimum time unit which can be counted by the device having the clock function, exactly the same time variable data is used for the preceding access and the present access. Accordingly, the content of the authentication data for the preceding log-in is exactly the same as that of the authentication data for the present access. In such a case, there is an inconvenience that a third person who eavesdropped the authentication data used for the preceding access during the transfer immediately logs in using the same authentication data to perform illegal access. Even if log-in is not performed consecutively within a minimum time unit which can be counted by the device having the clock function, there are cases where the tolerable error which is set for the time variable data as a common factor used at both sides in consideration of a slight error can be fulfilled. When such an error is considered, similar inconveniences occur when log-in is performed consecutively in a time range corresponding to the tolerable range. According to the second invention, a determination of appropriateness is made possible by the determination step on the conditions that it is determined that a prescribed interval time has been passed since the preceding access up to the present access. Thus, the inconvenience based on the illegal act of logging in consecutively using the same authentication data can be prevented to a maximum degree. According to the third invention, the authentication data is changed while maintaining the synchronization between the to-be-authenticated side and the

authenticating side. The authentication data is updated in synchronization by utilizing, as the common factor, time variable data which varies in accordance with an objective parameter of time, which is common nationwide. Accordingly, the above-described inconvenience of the log-in number synchronization system that the commonly changing data of both sides are put out of synchronization can be prevented to a maximum degree. Since the error in the time variable data caused by the malfunction of the clock means is automatically corrected, the inconvenience that the errors in the time variable data are gradually accumulated and the both sides are put out of synchronization can be prevented to a maximum degree. According to the fourth invention, the authentication data is changed while maintaining the synchronization between the to-be-authenticated side and the authenticating side. The authentication data is updated in synchronization by utilizing, as the common factor, time variable data which varies in accordance with an objective parameter of time, which is common nationwide. Accordingly, the above-described inconvenience of the log-in number synchronization system that the commonly changing data of both sides are put out of synchronization can be prevented to a maximum degree. Since a determination of appropriateness is made possible by the determination means on the conditions that it is determined that a prescribed interval time has been passed since the preceding access up to the present access, the inconvenience based on the illegal act of logging in consecutively using the same authentication data can be prevented to a maximum degree. According to the personal calculation apparatus of the fifth invention, the authentication data is changed while maintaining the synchronization between the to-be-authenticated side and the authenticating side. The authentication data is generated using time variable data which varies in accordance with an objective parameter of time, which is common nationwide, and output outside. Accordingly, the authenticating side determines

whether or not the output authentication data is appropriate or not and performs authentication, using the time variable data which varies in accordance with time. Thus, it is possible to update the authentication data in synchronization by utilizing, as the common factor, the time variable data which commonly changes nationwide. The above-described inconvenience of the log-in time synchronization system that the commonly changing data are put out of synchronization can be prevented to a maximum degree. Since the present time is displayed utilizing the counting operation of the clock function of the personal calculation apparatus, the person owning the personal calculation apparatus can recognize the present time with reference to the display, which improves the convenience. Even if the clock function malfunctions, the error can be easily recognized by referring to the display of the present time. According to the personal calculation apparatus of the sixth invention, the authentication data is changed while maintaining the synchronization between the to-be-authenticated side and the authenticating side. The authentication data is generated using time variable data which varies in accordance with an objective parameter of time, which is common nationwide, and output outside. Accordingly, the authenticating side determines whether or not the output authentication data is appropriate or not and performs authentication, using the time variable data which varies in accordance with time. Thus, it is possible to update the authentication data in synchronization by utilizing, as the common factor, the time variable data which commonly changes nationwide. Thus, the personal calculation apparatus which can prevent, to a maximum degree, the above-described inconvenience of the log-in time synchronization system that the commonly changing data are put out of synchronization can be provided. Since the time variable data, which is obtained by the counting operation performed utilizing the standard time which is obtained by the received standard time radio wave by the code/data

broadcasting is used as the commonly changing data, the authentication data can be generated by utilizing the time variable data which is more accurate and objective in accordance with the nationwide standard time. Thus, the personal calculation apparatus which can further improve the reliability of authentication on the authenticating side can be provided. According to the authentication apparatus of the seventh invention, the authentication data is changed while maintaining the synchronization between the access demanding side and the authenticating side. Authentication is performed by determining whether or not the authentication data transferred from the to-be-authenticated side is appropriate or not by utilizing, as the commonly changing data, time variable data which varies in accordance with an objective parameter of time, which is common nationwide. Accordingly, the to-be-authenticated side generates the authentication data using the time variable data as the commonly changing data and transfers the data. Thus, the authentication data can be updated in synchronization utilizing, as the common factor, the time variable data which varies in accordance with an objective parameter of time, which is common nationwide. Therefore, the above-described inconvenience of the log-in number synchronization system that the commonly changing data of both sides are put out of synchronization can be prevented to a maximum degree. Since a determination of appropriateness is made possible on the conditions that it is determined that a prescribed interval time has been passed since the preceding access up to the present access. Thus, the inconvenience based on the illegal act of eavesdropping the authentication data during transfer and logging in consecutively using the same authentication data can be prevented to a maximum degree.

[Brief Description of the Drawings]

[Figure 1] A perspective view.

[Figure 2] A flowchart.

[Figure 3] A function illustrating view.
[Figure 4] A function illustrating view.
[Figure 5] A function illustrating view.
[Figure 6] A perspective view.
[Figure 7] A flowchart.
[Figure 8] A flowchart.
[Figure 9] (A) and (B) are each a flowchart.
[Figure 10] A control circuit configuration of a personal terminal device.

[Description of the Reference Numerals]
3 is a personal terminal device; 2 is an input device; 1 is a keyboard; 33 is a wrist watch as an example of the personal calculation device; 13 and 14 are computers as an example of the determination means; 25 is a transmitter.

Japanese Patent No. 2835433

Fig.1

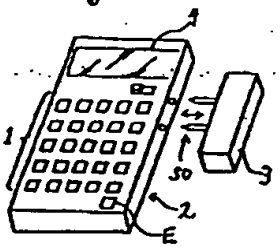


Fig.6

Fig.10

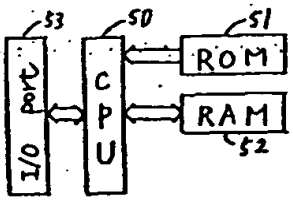


Fig.5

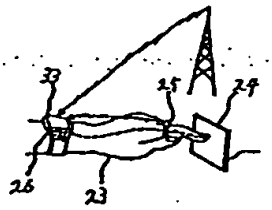


Fig.2

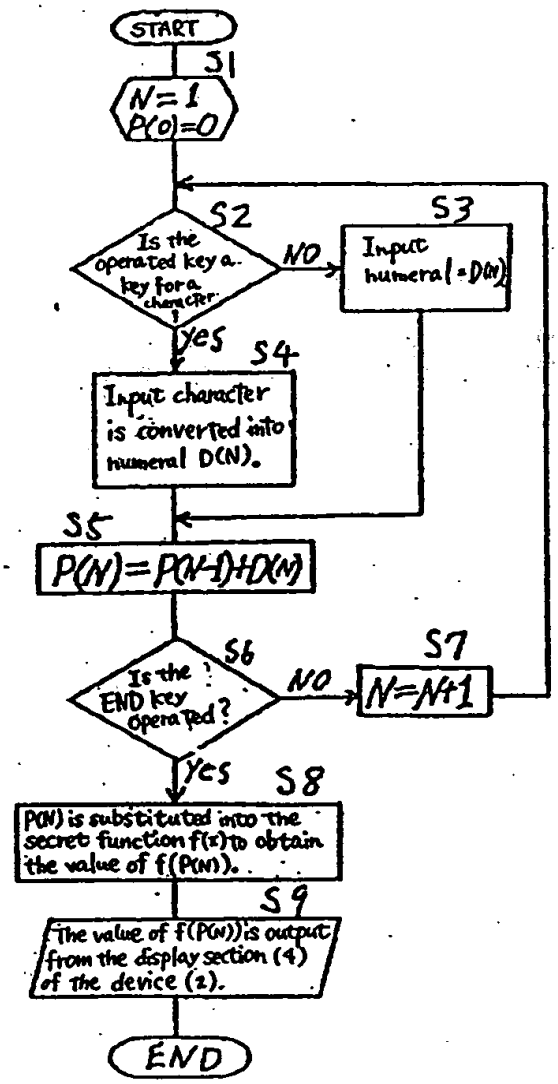


Fig.3

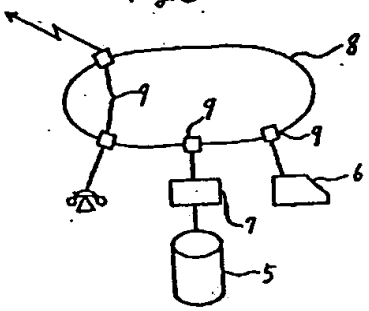
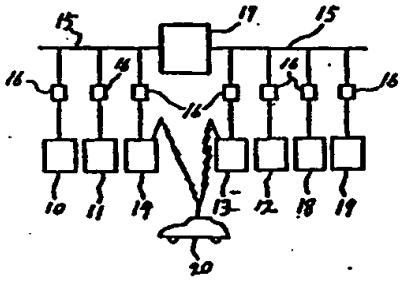
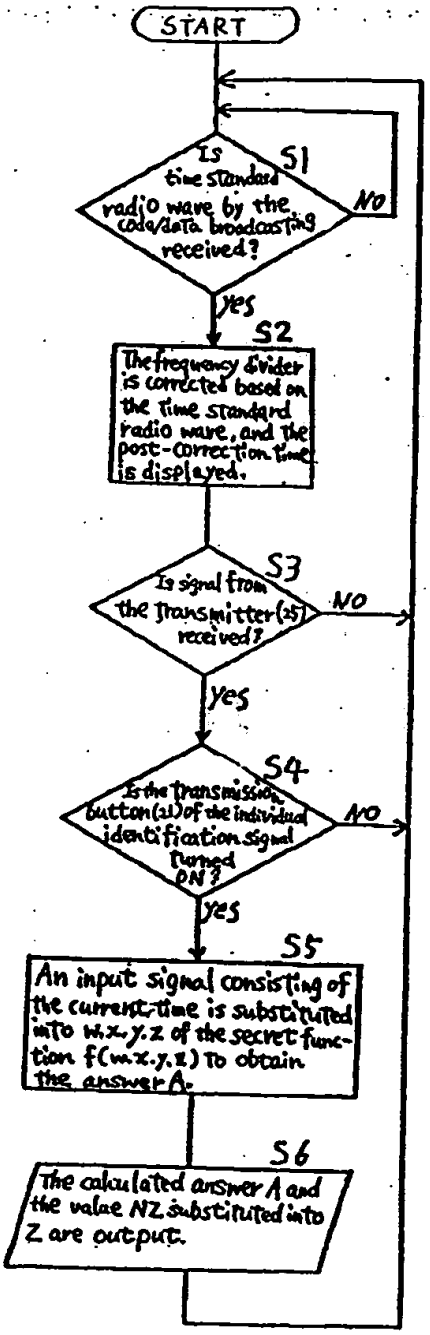


Fig.4



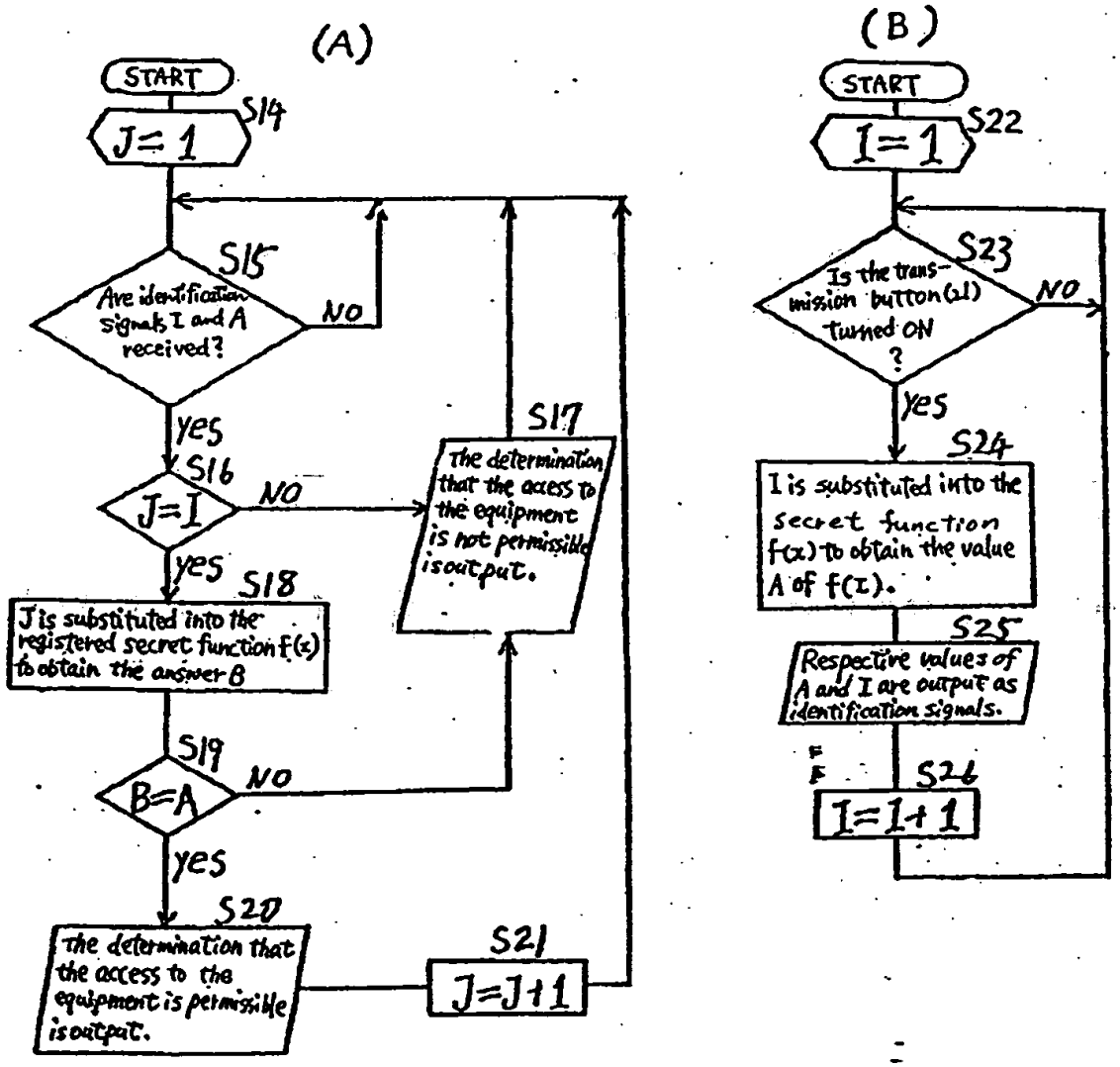
Japanese Patent No. 2835433

Fig. 7



Japanese Patent No. 2835433

Fig. 9



SHUSAKU YAMAMOTO

Re: Japanese Patents 2835433 and 2884338 of Fujiwara

Patent No. 2835433

<Indication>

Indication No. 1

Items registered

Filing date: October 11, 1984

Application number: 08-056966

Date of allowance: August 13, 1998

Number of inventions: 7

Title of the Invention: Access control method, and authentication system and device

Registration date: October 9, 1998

<Records on issue fee>

Issue fee

Year 1: 58,800 yen, paid on September 3, 1998

Year 2: 58,800 yen, paid on September 3, 1998

Year 3: 58,800 yen, paid on September 3, 1998

<Ownership>

Items registered

1st owner:

Yutaka TSUKAMOTO

40-15, Oaza Kitano, Oyodo-cho, Yoshino-gun

Nara-ken

Registration date: October 9, 1998

2nd owner:

[Transfer of the right]

Acceptance date: April 8, 1999

Acceptance number: 001200

822-2, Tsuchigahara, Tamano-shi, Okayama-ken

Kaneko FUJIWARA

Registration date: April 28, 1999

SHUSAKU YAMAMOTO

Re: Japanese Patents 2835433 and 2884338 of Fujiwara

3rd owner:

[Partial transfer of the right]
Acceptance date: August 30, 1999
Acceptance number: 003184
35-2, 5-chome, Utsukushigaoka, Aoba-ku,
Yokohama-shi, Kanagawa-ken
Kabushiki Kaisha Laurel Intelligent Systems
Registration date: September 24, 1999

October 29, 1999

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☑ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.